

Curs 5

## Struct Alg. în Informatică

- Pentru  $a, b \in \mathbb{Z}$ ,  $\gcd(a, b)$  și algoritmul Alg lui Euclid.

→  $\gcd(a, b)$  este determinat până la o asociere în diviziabilitate, ie până la semn.

$$\gcd(4, -6) = \pm 2$$

- De obicei, convenim să alegem  $\gcd$ -ul să fie valoarea  $> 0$ .

- Alg lui Euclid furnizează  $\gcd(a, b) \geq 0$

Lău exceptia cazului  $b=0$  și  $a < 0$

Def: Dacă  $\gcd(a, b) = 1$ , spunem că numerele  $a$  și  $b$  sunt prime între ele (coprime).

Proprietăți: Zie  $a, b, c \in \mathbb{Z}$

(1)  $\gcd(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}$  a.t.  $ua + vb = 1$

Denum: "Alg lui Euclid extins găsim  $u, v \in \mathbb{Z}$

"Denum:  $u, v \in \mathbb{Z}$  a.t.  $1 = \gcd(a, b) = ua + vb$

"C=" Stăm  $ua + vb = 1$ . Dacă  $d$  - divizor comun

pt  $a$  și  $b \Rightarrow d \mid ua + vb = 1 \Rightarrow d = \pm 1 \Rightarrow \gcd(a, b) = 1$

(2) Nu totdeauna  $d = \gcd(a, b)$ . Astunci  $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Denum: Conform Alg. Euclid  $\exists u, v \in \mathbb{Z}$

$$u \cdot a + v \cdot b = d \mid \frac{a}{d}$$

$$u \frac{a}{d} + v \frac{b}{d} = 1 \Rightarrow \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

$u \in \mathbb{Z}$      $v \in \mathbb{Z}$

③ Sei  $\text{pp. co } a, b \neq 0$ . Atunci:

$$\gcd(a, b) = \min \{ ua + vb \mid u, v \in \mathbb{Z}, ua + vb \geq 0\}$$

dem.:  $\forall m \in \mathbb{Z} \setminus \{0\}, \exists m = \min A$

concl. Euclid  $\Rightarrow \gcd(a, b) \in A \Rightarrow c \leq m \leq \gcd(a, b)$

$0 < \gcd(a, b)$  divide pe  $ua + vb \Rightarrow 0 < \gcd(a, b) \mid m$

$$\Rightarrow \gcd(a, b) \leq m \Rightarrow m = \gcd(a, b)$$

$$④ \quad \gcd(ac, bc) = c \cdot \gcd(a, b)$$

dsm:

$$\{ua \cdot ac + vb \cdot bc \mid u, v \in \mathbb{Z}\} = c \{ua + vb \mid u, v \in \mathbb{Z}\}$$

$\downarrow$   
 $c(ua + vb)$

$$⑤ \quad \Rightarrow \gcd(ac, bc) = c \cdot \gcd(a, b)$$

$$\Rightarrow \gcd(ac, bc) = c \cdot \gcd(a, c) = 1 \Rightarrow \gcd(a, bc) = 1$$

⑤ Dacă  $\gcd(a, b) = \gcd(a, c) = 1 \Rightarrow \gcd(a, bc) = 1$

dsm Euclid  $\Rightarrow \begin{cases} 1 = ua + vb \\ 1 = u_1 a + v_1 c \end{cases} \quad u, v, u_1, v_1 \in \mathbb{Z}$

$$\Rightarrow 1 = u \cdot u_1 \cdot a^2 + uv_1 \cdot a \cdot c + u_1 \cdot v \cdot ab + v \cdot v_1 \cdot b \cdot c$$

$$+ uv_1 \cdot bc \stackrel{(1)}{\Rightarrow} \gcd(a, bc) = 1$$

$1 = a(uv_1)$      $uv_1 \in \mathbb{Z}$

Atunci  $a \mid bc$  și  $\gcd(a, b) = 1$ , atunci  $a \mid c$

$$⑥ \quad \text{dacă } a \mid bc \text{ și } \gcd(a, b) = 1 \text{ atunci } 1 = ua + vb \mid c$$

dsm  $\exists u, v \in \mathbb{Z}$  a.t.  $1 = ua + vb \mid c$

$c = \underbrace{u \cdot ac}_{:a} + \underbrace{v \cdot bc}_{:a} = a \mid c$

⑦ Dacă  $c \neq 0$  și  $a \cdot c | b \cdot c$ , atunci  $a | b$

Dacă:  $b \cdot c = a \cdot k$  cu  $k \in \mathbb{Z}$  și  $\frac{1}{c} \neq 0$

$$\Rightarrow b = a \cdot k \text{ cu } k \in \mathbb{Z} \Rightarrow a | b$$

Prop Fixează  $a, b, c \in \mathbb{Z}$ . Atunci  $\text{lcm}(a, b) \cdot \text{gcd}(a, b)$   
 $= ab$

Dacă nu este  $d = \text{gcd}(a, b) \Rightarrow$  avem  $a = d \cdot a_1$ , și  $a_1, b_1 \in \mathbb{Z}$   
 $b = d \cdot b_1$ ,  $\text{gcd}(a_1, b_1) = 1$

Xor  $L = \boxed{d \cdot a_1 \cdot b_1} = a \cdot b_1 = a \cdot b$ , deci  $L = \text{mult. comun } a, b$

Fixează  $m \in \mathbb{Z}$  - mult. comun al lui  $a$  și  $b \Rightarrow$

$\Rightarrow m = a \cdot m_1$ , cu  $m_1 \in \mathbb{Z}$  deci  $d \cdot b_1 | d \cdot a_1 \cdot m_1 \Rightarrow$

iar  $b_1 | m$

$d \cdot b_1 | "a \cdot m_1 = d \cdot a_1 \cdot m_1$

$\Rightarrow b_1 | a_1 \cdot m_1$

$\text{gcd}(a_1, b_1) = 1$   
 $\Rightarrow b_1 | m_1 \Rightarrow m_1 = b_1 \cdot m_2$  cu  $m_2 \in \mathbb{Z} \Rightarrow$   
 $\Rightarrow m = 0 \cdot m_1 = a \cdot b_1 \cdot m_2 = L \cdot m_2 \stackrel{\text{def}}{=} L = \text{lcm}(a, b)$

Verificare:  $L \cdot d = \underbrace{d \cdot a_1}_{a} + \underbrace{b_1 \cdot d}_{b} = a \cdot b$

Numeri primi:

Dif:  $jm$  și un număr  $p \neq 0, \pm 1$ ,  $\exists n$  prim dacă și numai dacă există produs de numere întregi  $\neq \pm 1$   
 $p = a \cdot b$  și  $b \neq 0 \Rightarrow a = \pm 1$  sau  $b = \pm 1$   
dacă  $m \in \mathbb{Z} \setminus \{0, \pm 1\}$  nu este prim, sau numărul  $n$   
este număr compus.  
ex:  $2, 3, 5, 7, 11, \dots$  numere prime

Mersenne:  $M_m = 2^m - 1$  cu  $m$  prim

$$M_2 = 2^2 - 1 = 3$$

$$M_3 = 2^3 - 1 = 7$$

$$M_5 = 2^5 - 1 = 31$$

$$M_7 = 2^7 - 1 = 127$$

--- etc

în 2023:  $M_{82589933}$  este nr. prim

OBS: Fie  $p \in \mathbb{Z}$  prim. Pentru  $a \in \mathbb{Z}$ .  $\gcd(a, p) = 1 \Leftrightarrow$

$$\Leftrightarrow p \nmid a$$
 sau  $\gcd(a, p) = p \Leftrightarrow p \mid a$ 

Teorema Fie  $p \in \mathbb{Z} \setminus \{0, \pm 1\}$ . Asumej:

$p$ -prim  $\Leftrightarrow (\forall a, b \in \mathbb{Z} \quad p \mid ab \Rightarrow p \mid a$  sau  $p \mid b)$

din „ $\Rightarrow$ ”  $p_p \cdot p$  prim. Fie  $a, b \in \mathbb{Z}$  cu  $p \nmid ab$ .

Dacă  $p \nmid a$

Dacă  $p \nmid a \Rightarrow \gcd(a, p) = 1 \Rightarrow p \mid b$

„ $\Leftarrow$ ”  $p_p \cdot c \bar{p}$  nu e prim  $\Rightarrow \exists a, b \in \mathbb{Z}$  cu  $p = ab$

$|a|, |b| \neq 1 \Rightarrow |a|, |b| \geq 2 \Rightarrow p \mid ab \stackrel{ip}{\Rightarrow} p \mid a$  sau  $p \mid b$

$p \neq 0 \quad |p| \leq |a|$

$a, b \neq 0 \quad |p| \leq |b|$

$|p| = |a| \cdot \underbrace{|b|}_{\geq 2} \Rightarrow |p| \neq 1$  și  $|p| > |b|$

Așadar  $p$  prim

Teorema: (Euclid) Orice număr  $n \in \mathbb{Z}$ ,  $n \neq 0, \pm 1$ , se poate scrie ca produs de factori primi în  $\mathbb{Z}$

Ora mea  $n = p_1^{d_1} \cdot p_2^{d_2} \cdots p_t^{d_t}$  unde  $p_i$  sunt factori primi.

Acompanierea este unuă până la o reordonare a termenilor și a semnelor.

$$n = \pm p_1^{d_1} \cdot p_2^{d_2} \cdots p_t^{d_t} \quad \text{cu } p_1, p_2, \dots, p_t \text{ sunt prime distincte}$$

$$d_1, d_2, \dots, d_t \in \mathbb{N}^*$$

$$\text{ex: } 60 = 2^2 \cdot 3^1 \cdot 5^1$$

$$-60 = -2^2 \cdot 3^1 \cdot 5^1 = -2^2 (-3) (-5)$$

DIM: Există: Fie  $n \in \mathbb{Z}, n \neq 0, \pm 1$ ,  $|n| \geq 2$

Dacă  $n$  primă  $\rightarrow$  OK

Dacă  $n$  nu e prim  $\Rightarrow n = ab$  cu  $a, b \neq \pm 1$

$$2 \leq |a| \leq |n|$$

Alăturăm descompunerea pt.  $a$  și pt  $b$  ca produs de nr. prime și obținem o descompunere pt  $n$ ! ca produs de prime.

Unicitatea: Teorema prin inducție după  $n$

Teorema: (Euclid) Există o infinitate de nr. prime.

DIM: Primă  $P$ . A se presupune că  $P_1, P_2, \dots, P_t$  sunt toate nr. prime

$$\text{Fie } N = P_1 \cdot P_2 \cdots \cdot P_t + 1 > P_i, \forall i=1, t$$

# Pi XIX vi

Contradictie: cu existenta descompunerii lui  $x$  ca produs de numere prime.

Teorema: (Hardy - Littlewood, ~1944)

Notam: cu  $\pi(x)$  = numarul numerelor prime in  $[0, x]$  pt  $x \in \mathbb{N}^+$ .

$$\text{Atunci } \pi(x) \approx \frac{x}{\ln x}$$

Propozitie: Fix  $m \in \mathbb{Z}^+ \setminus \{1, \pm 1\}$  cu divizorii in factori primi  $n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t}$  cu  $p_i > 0$  prime distincte, toti  $\alpha_i > 0$ .

Atunci orice divizor al lui  $n$  este de forma:

$$\pm p_1^{\beta_1} p_2^{\beta_2} \dots p_t^{\beta_t} \text{ cu } \beta_i \text{ cu } 0 \leq \beta_i \leq \alpha_i,$$

$$\forall i = 1, t$$

In particular  $m$  are  $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_t + 1)$  divizori pozitivi.

Dlm: Dacă  $x \in \mathbb{N}$  și  $x | m = \pm p_1^{\alpha_1} \dots p_t^{\alpha_t} \Rightarrow$

$$\Rightarrow m = xg \text{ cu } g \in \mathbb{Z}$$

Pentru ca ea div. lui  $x$  și a lui  $g$  au factori primi comunii (unica), div. a lui  $m$  corespunde unui produs de factori primi.

Th: Fix  $p_1, p_2, \dots, p_t$  factori primi care apar in descompunerile pt a ramurilor  $\mathbb{Z} \setminus \{0, \pm 1\}$

$$- a = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t} \text{ cu } \alpha_i \in \mathbb{N}_{i=1,t}$$

$$b = \pm p_1^{\beta_1} \cdots p_t^{\beta_t} \text{ cu } \beta_i \in \mathbb{N}$$

Akunca:  $\gcd(a, b) = \prod_{i=1}^t p_i^{\min\{\alpha_i, \beta_i\}}$

$$\operatorname{lcm}(a, b) = \prod_{i=1}^t p_i^{\max\{\alpha_i, \beta_i\}}$$

Sistem  $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$

x  $x+y = \max\{x, y\} + \min\{x, y\}$